National Infrastructure Protection Center CyberNotes

Issue #17-99 *August 18, 1999*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between August 1 and August 13, 1999. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Acushop (Red Hat Linux 6.0[1])	SalesBuilder	Acushop SalesBuilder is an E-Commerce program included as a demo in the Red Hat Linux 6.0 applications CD. The startup file .sbstart linked from usr/bin/salesbuilder and /sur/local/bin/salesbuilder is set world writable. This allows attackers to modify the file and add malicious commands, which could lead to a local root compromise.	No workaround or patch available at time of publishing.	Acushop Salesbuilder Demo Compromise	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Allaire (Windows NT[2])	ColdFusion	ColdFusion Server includes several undocumented CFML tags and functions that are used in the ColdFusion Administrator. As a result, developers who have permission to create Web applications and executable ColdFusion templates on a ColdFusion server can make use of the undocumented functions and tags to potentially gain unauthorized access to administrative settings including registry, database and advanced security settings.	No patch or workaround available at time of publishing.	CFML Tag Vulnerability	**High**	Bug discussed in newsgroups and websites.
Cisco 675[3]	Cisco 675 Asymmetric Digital Subscriber Line (ADSL) Router	Cisco 657 routers that aren't password protected can be compromised to give you have full access to all the router's settings.	This is fixed in 2.1.0a or in 2.2.0 (2.2.0 out shortly).	CISCO 675 Password Vulnerability	Medium/ Low	Bug discussed in newsgroups and websites. **Exploiting the flaw requires no special tools or knowledge.**
CREAR (Windows 95, 98, NT 4.0[4])	AlMail32 1.10	The ALMail32 POP3 client contains a buffer overflow. An abnormally long FROM: or TO: field in the header of an incoming e-mail will overwrite the buffer and allow arbitrary code to be executed.	Currently no workaround or patch available at time of publishing.	Mail POP3 Buffer Overflow Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[1] Security-Focus, August 3, 1999.
[2] NTBugtraq, July 30, 1999.
[3] Bugtraq, August 3, 1999.
[4] Security-Focus, August 9, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Debian[5]	Cfingerd before 1.4.0	In certain configurations, a vulnerability exists that enables any local user to execute arbitrary programs with root privileges.	Recommended Action: Immediately turn off ALLOW_EXECUTION in your cfingerd.conf file then upgrade to the most recent version of cfingerd 1.4.0 which can be found at: ftp://metalab.unc.edu/pub/Linux/system/network/finger/	Debian Cfingerd Allow_ Execution Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Debian[6] *This is a new Samba 2.0.5a software package release that addresses vulnerabilities identified in previous CyberNotes.*	Debian GNU/Linux 2.1	Samba 2.0.5a has been released which addresses the following security vulnerabilities: - A DoS attack could be performed against the netbios name daemon (nmbd). - a buffer overflow was present in the message service in smbd - a race condition in smbmnt allowed users to mount at arbitrary points of the file system if submnt is setuid	These problems have been fixed in version 2.0.5a-1. Upgrade your samba packages immediately. Please note that this is a major upgrade so please be careful when you upgrade since some changes to the configuration file might be necessary. The configuration file has also moved to a new location (/etc/samba). The smbfsx package is also obsolete with this update and has been replaced by smbfs, which can handle both 2.0 and 2.2 kernels now. wget ur l will fetch the file for you dpkg -i file.deb will install the referenced file.	Various Security Vulnerabilities	Low/ Medium/ High (Multiple vulnera-bilities addressed)	Bug discussed in newsgroups and websites.
FlowPoint DSL routers[7] ***This is a new FlowPoint firmware package release that addresses vulnerabilities identified in pervious versions 3.0.2 through 3.0.7***	FlowPoint versions 3.0.2 through 3.0.7	Vulnerability exists that allows a password recovery feature to be utilized from the LAN or WAN instead of just the serial console port. Basically, throwing enough 6 digit numbers at a pre-3.0.8 router will allow you to get access to the box to do whatever you want.	Upgrade your routers to the latest version, 3.0.8 or later from FlowPoint's FTP site: http://www.flowpoint.com/support/techbulletin/sec308.htm **Warning:** Make sure that you access the correct directory for your router. Loading the incorrect firmware on the router can result in an inoperable router.	FlowPoint Router Password Vulnerability	**High**	Bug discussed in newsgroups and websites**.**

[5] Bugtraq, August 10, 1999.
[6] Bugtraq, August 1, 1999.
[7] Bugtraq, August 7, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
FreeBSD, OpenBSD, NetBSD, BSD/OS[8]	BSD 4.4 based operating systems	Several security holes have been discovered to be the result of programmers' not checking return values of system calls. There is a condition that might make chmod() or chown() fail if BSD file flags are set. The superuser must explicitly clear these flags before the system calls can succeed. There are several implications of the problem, which range from Denial of Service attacks to actual exploitation.	FreeBSD: For the latest information on this issue (FreeBSD-SA-99:01) http://www.freebsd.org/security NetBSD: Only NetBSD/current has been fixed. BSDI: ftp://ftp.bsdi.com/bsdi/patches/patches-4.0.1/M401-014 ftp://ftp.bsdi.com/bsdi/patches/patches-3.1/M310-056 OpenBSD: http://www.openbsd.org/security.html#25 Xfree: They are currently working on a fix.	BSD File Flags and Programming Techniques	Medium/ High	Bug discussed in newsgroups and websites.
Fujitsu (Windows 95, 98, NT 3.5.1, NT 4.0[9])	Chocoa 1.0beta7R	The Chocoa IRC client contains a buffer overflow that may allow an unauthorized user to execute arbitrary code on the client system.	Currently no patch or workaround available at time of publishing.	Chocoa IRC Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Linux[10]	Linux kernel 2.0.30, 2.0.35, 2.0.36, 2.0.37	Certain Linux kernels in the 2.0.3x range are susceptible to blind TCP spoofing attacks. For this vulnerability to be effective, 3 conditions have to be met: The spoofed machine must be off the network or incapable of sending data out/receiving data properly; the target machine must not be communicating actively with any other machines at the time; and no packets between the attacker's machine and the target can be dropped during the attack.	This issue was patched in kernel 2.0.33 and fixed in 2.0.34 but the problem was re-introduced in 2.0.36 No workaround or patch available at time of publishing.	Blind TCP Spoofing Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[8] Bugtraq, August 5, 1999.
[9] Security-Focus, August 9, 1999.
[10] Bugtraq, August 1, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[11]	Commercial Internet System 2.0, 2.5; IIS 4.0; Site Server 3.0 Commerce Edition; Site Server 3.0	Microsoft IIS and all products that use the IIS web engine have a vulnerability whereby a flood of specially formed HTTP request headers will make IIS consume all available memory on the server. IIS activity will be halted until the flood ceases or the service is stopped and restarted.	Microsoft released a patch for this vulnerability on August 11th (MS99-028). **However, on August 12, they retracted it due to an error that made IIS hang whenever the logfile was an exact multiple of 64KB. A new patch will be released shortly.** (See Microsoft Security Bulletin (MS99-029) located at: www.microsoft.com/security/bulletin/MS99-029.asp	Malformed HTTP Request Header Vulnerability	Low	Bug discussed in newsgroups and websites.
Microsoft[12]	Exchange 4.0, 5.0, & 5.5	A vulnerability exists that allows a malicious user to perform mail relaying via an Exchange Server that is configured to act as a gateway for other Exchange sites using the Internet Messaging Service.	A patch has been released for Microsoft Exchange Server 5.5: ftp://ftp.microsoft.com/bussys/exchange/exchange-public/fixes/Eng/Exch5.5/PostSP2/imc-fix	Encapsulated SMTP Address Vulnerability	Medium	Bug discussed in newsgroups and websites.
Microsoft Windows 95[13]	FrontPage PWD32/3.0.2.926	FrontPage Server crashes when the URL is 167+ characters long.	No workaround or patch available at time of publishing.	Front Page DoS Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft Windows 95.0a & 95.0b, 98 & 98.0se, 2000; SunOS; Solaris 2.6, 2.6_ x86[14]	Microsoft ICMP Router Discovery Protocol	The ICMP Router Discovery Protocol (IRDP) does not have any form of authentication, making it impossible for end hosts to tell whether or not the information they receive is valid. Because of this attackers can perform a number of attacks from web page hacks to stealing credentials or modifying/altering data. **Most cable modem DHCP clients and large internal organizations are at risk. Because of the large number of vulnerable systems, and the fact that this attack will penetrate firewalls that do not stop incoming ICMP packets, this Denial of Service attack can become quite severe.**	Windows95/98: Microsoft Knowledge Base contains an article that gives information on how to disable IRDP, it can be found at: http://support.microsoft.com/support/kb/articles/q216/1/41.asp Solaris: Configure your host to obtain a default gateway through DHCP, static routes, or via the /etc/defaultrouter file. Firewalls: Block all ICMP Type 9 & Type 10 packets. This should protect against remote DoS attacks.	ICMP Router Discovery Protocol Vulnerability	Low/ Medium/ **High**	Bug discussed in newsgroups and websites. Exploit has been published

[11] Security-Focus, August 11, 1999.
[12] Bugtraq, August 7, 1999.
[13] Bugtraq, August 7, 1999.
[14] Security-Focus, August 12, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows NT[15]	Windows NT Server 4.0, Terminal Server Edition	A remote attacker can mount a Denial of Service attack by levying a large number of bogus connection requests and consuming all memory on the Terminal Server.	Microsoft has issued a patch that eliminates this vulnerability located at: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40tse/hotfixes-postSP4/Flood-fix	TSE Bogus Request Flooding Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
NetBSD prior to 1.4.1[16]	Operating System (Profil(2))	Profil(2) can modify setuid root programs.	Upgrade to NetBSD 1.4.1, NetBSD-current.	NetBSD Profil(2) Vulnerability	**High**	Bug discussed in newsgroups and websites.
Network Associates (Solaris 2.6 and BSDI[17])	Gauntlet 5.0 Firewall	Sending specially crafted packets to/through the firewall can cause it to lock up. Each site should access whether systems protected by Gauntlet 5.0 Firewall are mission critical.	Network Associates just released a patch for the problem. It can be found at: ftp://ftp.tis.com/gauntlet/patches/5.0	Gauntlet Firewall Denial of Service Vulnerability	**High** (Due to the potential systems affected)	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the Press.
Network Security wizards[18]	Dragon-Fire IDS remote web interface under version 1.0	The remote web interface has an insecure CGI script, which allows users to remotely execute commands as the user nobody. This could lead to a remote compromise of the system.	Modify Dragon-Fire exposed to the internet in the following manner: Open dfire.cgi with vi. Goto to line 215 with a ':215' command. The line should read: $command = $command .'-f' .$db . $input{'database'} . '/dragon.db'; It may be slightly off if you have modified the dfire.cgi.script. Below that line please add the following two lines: $AOK = '-a-zA-ZO-9_.+:/'; $command =~ s/[^$AOK]/ /go; Verify that the new Dragon-Fire works by performing a few queries.	Dragon-Fire IDS Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Qident[19]	IRCD2.10.x	Efnet IRCD Hybrid-6 (up to beta 58) has a vulnerability that can allow remote access to the IRC server. In most cases, you'll gain privileges of "irc" user.	No workaround or patch available at time of publishing.	Qident IRDC Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[15] Microsoft Security Bulletin (MS99-028), August 9, 1999.
[16] NetBSD Security Advisory 1999-011, August 9, 1999.
[17] Bugtraq, August 6, 1999.
[18] Security-Focus, August 5, 1999.
[19] Bugtraq, August 8, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Ramp Networks[20]	WebRamp 200i1.0 & M31.0	The setup program in WebRamp does not force you to change the default password. When you connect to some WebRamp servers on an ISP, they already tell you the username to use and password. A malicious user would have the ability to change the routing table and firmware. On systems with more than one modem attached, it is possible to have one modem call a remote computer, providing outside access to the internal LAN.	The wradmin password should be changed at installation	WebRamp Password Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Red Hat Linux 5.2 & 6.0, all architectures [21]	Operating System	The CGI program can be used remotely as a powerful portscanning or a Denial of Service tool .	Red Hat Linux 6.0: Intel: ftp://updates.redhat.com/6.0/i386/squid-2.2.STABLE4-5.i386.rpm Alpha: ftp://updates.redhat.com/6.0/alpha/squid-2.2.STABLE4-5.alpha.rpm Sparc: ftp://updates.redhat.com/6.0/sparc/squid-2.2.STABLE4-5.sparc.rpm Source packages: ftp://updates.redhat.com/6.0/SRPMS/squid-2.2.STABLE4-5.src.rpm Red Hat Linux 5.2: Intel: ftp://updates.redhat.com/5.2/i386/squid-2.2.STABLE4-0.5.2.i386.rpm Alpha: ftp://updates.redhat.com/5.2/alpha/squid-2.2.STABLE4-0.5.2.alpha.rpm Sparc: ftp://updates.redhat.com/5.2/sparc/squid-2.2.STABLE4-0.5.2.sparc.rpm Source packages: ftp://updates.redhat.com/5.2/SRPMS/squid-2.2.STABLE4-0.5.2.src.rpm	Red Hat Cachemgr.CGI Vulnerability	Low	Bug discussed in newsgroups and websites.

[20] Bugtraq, August 3, 1999.
[21] RHSA-199:025, July 30, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Sun[22]	CDE bundled with Solaris 2.6	A bug exists in stdcm_convert, which may be used to _create_ files owned by root, but writable by your group, which could result in a possible local root compromise.	A quick solution is to remove the setuid bit from stdcm_convert or remove/disable the program completely.	Stdcm_convert Vulnerability	**High**	Bug discussed in newsgroups and websites.
Sun Solaris 2.6, 2.7_x86; Slackware Linux 4.0; SuSE Linux 6.0; RedHat Linux 5.2; Debian Linux 2.1[23]	GNU Gnome 1.0	The Gnumeric spreadsheet program includes various plugins to implement functions from different programming environments into a spreadsheet. The Guile plugin was exporting a function that allows any user to run arbitrary scheme code.	Upgrade Gnumeric to the latest version at: ftp://ftp.gnome.org/pub/GNOME/sources/gnumeric	Guile Plugin Vulnerability	**High**	Bug discussed in newsgroups and websites.
WebTrends (Linux 2.2.x; Red Hat Linux 5.2, 6.0; Solaris 2.5.1, 2.6, 2.7[24])	Enterprise Reporting Server 1.5	Specifying a negative content-length in a POST operation will crash the web server.	No workaround or patch available at time of publishing.	Content Length DoS Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

[22] Bugtraq, August 9, 1999.
[23] Security-Focus, August 5, 1999.
[24] Bugtraq, August 8, 1999.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between August 1 and August 13, 1999, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 8 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
August 13, 1999	**Ircdexp.tgz**	**Remote access script that exploits IRCD vulnerability.**	
August 12, 1999	**Blindspoof.c**	**A script that exploits the blind TCP spoofing vulnerability.**	
August 10, 1999	**Doomzday4.c**	**Exploit script, which starts an IRC client with a spoofed ident.**	
August 9, 1999	**Ex_almail.c**	**Exploit script that will overwrite the buffer and allow arbitrary code to be executed against AlMail32 POP3 clients.**	
August 9, 1999	**Ex_chocoa.c**	**An exploit script against Fujitsu Chocoa that will open an instance of notepad on the target with the autoexec.bat file loaded into it.**	
August 8, 1999	**Wtkill.pl**	**A DoS script against WebTrends Enterprise Reporting Server that specified a negative content-length in a POST operation.**	
August 7, 1999	**DoS.pl**	**A DoS script that exploits a FrontPage vulnerability.**	
August 5, 1999	Gauntlet-dos.c	A DoS script that remotely locks up the firewall.	

Due to the potential security impact in Corporate Security Environment, we are including a table containing Back Orifice 2000 updates. **Items listed in boldface/red (if any) are new updates.**

Name	Description
BOTOOL.ZIP v1.0	BOTOOL is a point-and-click graphical interface to remotely manage files and the remote registry. The remote registry editor allows you full registry-editing capabilities over the BO2K secure command channel.
BO_CAST	A plugin for remote administration suite BO2K which fixes the password vulnerability..
IDEA version 0.4	A plugin which fixes the flaw which caused any password to generate the same key.

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While this section will list only short descriptions, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

Trends for this two week period:

1. Servers are being penetrated using the RDO exploits.
2. IIS vulnerabilities are being exploited.
3. Infrastructure attacks against corporate e-mail.
4. Weak passwords are becoming a security nightmare for large organizations.
5. Security holes in CGI scripts are currently being exploited.
6. An increased number of reports of SYN and IP Spoofing attacks that result in a Denial-of-Service.
7. Hackers have taken a greater interest in cable modems and DSL lines. Individual report receiving two probes per day against their machines using cable modems or DSL lines.

Viruses/Trojans

VBS.Monopoly: is a "Melissa-style" Internet worm. It spreads through e-mail using the MS Outlook client. The worm sends itself with a message to all addresses from the Outlook address book. The message contains the attached file "MONOPOLY.VBS". The VBE file contains encrypted VBScript and is executed with WSH file. When VBE is executed it displays the message:

Bill Gates is guilty of monopoly. Here is the proof

Then it displays a picture from the image file. The picture shows Bill Gates' face on Monopoly game board.

VBS.Monopoly also sends another message to the addresses:

monopoly@mixmail.com
monpooly@telebot.com
mooponly@ciudad.com.ar
mloponoy@usa.net
yloponom@gnwmail.com

In this message the worm sends a list of names and addresses from the Outlook address book, ICQ UIN files and information from Windows registry. After all that, the worm modifies the system registry:

"HKEY_LOCAL_MACHINE\Software\OUTLOOK.Monopoly\" = "True"

In this way the worm "marks" the computer and will not send messages with confidential information from this computer for a second time.

Spirit2000 versions Beta and 1.2 (August 7, 1999): The beta of this Trojan can upload/download files from your harddrive, grab ICG and other passwords, as well as a feature called 'Burn Monitor', which will constantly resets the screens resolution. The next version v1.2 can also do more netbus-like features, such as turn on/off your monitor, start button, taskbar, mouse, etc. This Trojan is for Windows 95/98 only and will not run under NT.

Vampire 1.0 (August 7, 1999): This is a basic Trojan with many standard features, however it does have some destructive features such as 'Format HD'. It runs on both Windows 95/98 and Windows NT.

SubSeven Apocolypse (August 7, 1999): This is the newest version of SubSeven with a revamped Client.

Matrix 1.4 (August 8, 1999): This is a Trojan that is based on sourcecode to Girlfriend Trojan. Its main feature is an FTP like file server and the ability to update the Trojan exe on a victim's computer to a newer version with a one-button click.